





Зарплата для Нео:

Однажды Нео  приняли на работу в корпорацию «ООО МАТРИЦА» директором которой являлся, чёрный хакер Морфиус . Он разглядел в Нео потенциал и дал пробное задание: Морфеус положил первую зарплату Нео в сейф, пароль от сейфа Морфеус зашифровал с помощью блочного алгоритма шифрования «SMITHetel» построенного на основе классической сети Фейстеля.

1 Блочный алгоритма шифрования SMITHetel

Пусть:

- V_l - это вектор из 0 и 1 длины $l \in \mathbb{N}$;
 - $Text = t_1 || t_2 || \dots || t_r$ - это текст который необходимо зашифровать, где:
 - $r \in \mathbb{N}$;
 - $t_i, t_2, \dots, t_{r-1} \in V_8$;
 - в случае если $t_r \in V_8$, то с текстом не происходит никаких дополнительных преобразований, если же длина блока t_r меньше 8 бит, то он дополняется нулями таким образом, чтобы длина t_r стала равна 8 битам.
- То есть текст который необходимо зашифровать последовательно разбивается на блоки по 8 бит, при этом если последний блок меньше 8 бит, то он дополняется нулевыми битами таким образом, чтобы его длина стала равна 8 бит.*

- $Key = k_1 || k_2 || \dots || k_{12}, k_i \in V_4, i = \overline{1, 12}$ - секретный ключ длины 48 бит.

Далее каждый блок текста t_i , где $i = \overline{1, r}$ шифруется с помощью функции E_K независимо от других, то есть зашифрованный текст выглядит следующим образом $s_1 || s_2 || \dots || s_r$, где $s_i = E_K(t_i)$.

1.1 Правила функционирования функции E_K .

Функция зашифрования $E_K : V_8 \rightarrow V_8$ при фиксированном ключе - это биективное отображение множества V_8 или другими словами E_K подстановка на байтах. Функция E_K - это последовательное применение 12 преобразований $e_{k_1}, e_{k_2}, \dots, e_{k_{12}}$. То есть

$$E_K(t) = e_{k_{12}} \circ e_{k_{11}} \circ \dots \circ e_{k_1}(t).$$

Опишем правила зашифрования одного Блока (байта) t с помощью одного раунда зашифрования e_k алгоритма *SMITHetel* на 4-ёх битном ключе k :

- Блок t разбивается на 2 блока по 4 бита - t_1 и t_2 ;
- Зашифрованный блока будет иметь вид $s = (s_1 || s_2) = ((t_2 \oplus F(k \oplus t_1)) || t_1)$

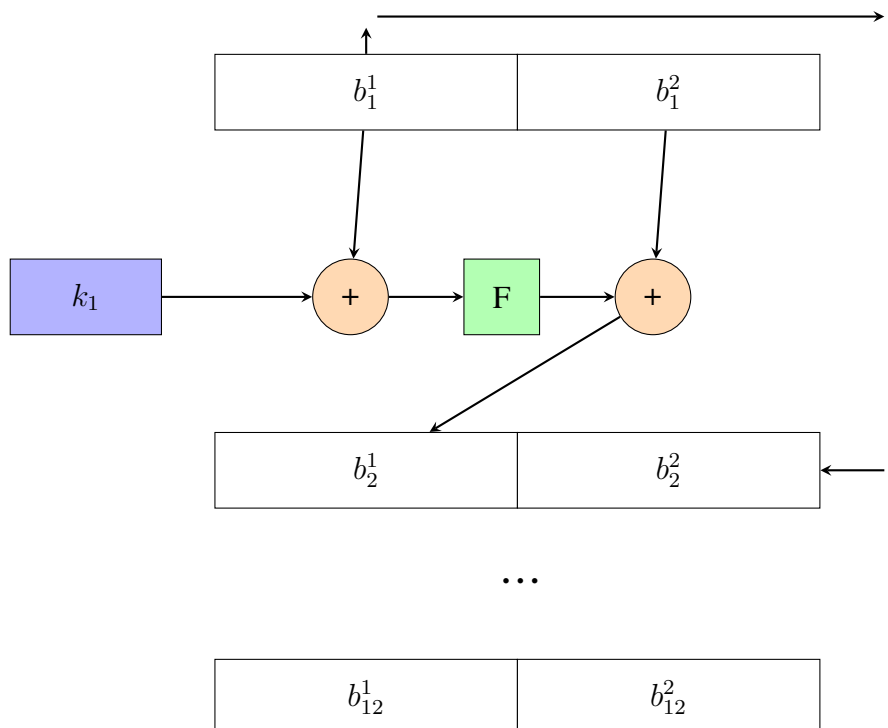


Функция $F : \{0,1\}^4 \rightarrow \{0,1\}^4$ - биекция и представляет из себя подстановку следующего вида:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 12 & 4 & 6 & 2 & 10 & 5 & 11 & 9 & 14 & 8 & 13 & 7 & 0 & 3 & 15 & 1 \end{pmatrix}$$

Это означает, что если на ей на вход подать любое 4ех битное число, то она возвращает новое 4ех битное число, согласно схеме выше. **Пример:** $F(3) = 2$

Схематичное представление алгоритма *SMITHetel*:



- это функция битового *xor* двух чисел



Дополнительные сведения:

Морфиус оставил Вам один пример: пару пароль (*pass*) и соответствующий шифрованный пароль ($E_K(pass)$) вашего коллеги, при этом ключ зашифрования и в Вашем случае и в примере ниже совпадают:

пароль: в битовом представлении:

1100101010110010101000101110000011001011100010101101010110111001₂;



зашифрованный пароль: в битовом представлении:

1100000111011110110011110010001100001000100110000001011001010110₂.

Помогите Нео найти его пароль если зашифрованный пароль в битовом представлении имеет вид:

1010111000000101001100101110111001101000111100010101010001011110₂.

После чего нужно преобразовать этот пароль в флаг следующим образом: $cyzi\{decode\ message\}$, где *decode message* это сообщение из 0 и 1 которое вы получили в процессе расшифровки. Это нужно послать в систему.